



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



020.301 CHFS Network-User Account Policy


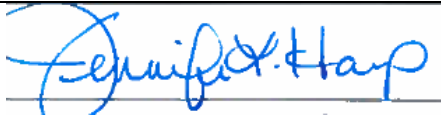


**Version 2.3
September 14, 2018**

020.301 CHFS Network-User Account Policy	Current Version: 2.3
020.300 Administrative Security	Review Date: 09/14/2018

Revision History

Date	Version	Description	Author
9/2/2002	1.0	Effective Date	CHFS OATS Policy Charter Team
9/14/2018	2.3	Review Date	CHFS OATS Policy Charter Team
9/14/2018	2.3	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
IT Executive (or designee)	9/14/2018		
CHFS Chief Information Security Officer (or designee)	8/20/2018		

020.301 CHFS Network-User Account Policy	Current Version: 2.3
020.300 Administrative Security	Review Date: 09/14/2018

Table of Contents

1	POLICY DEFINITIONS.....	4
2	POLICY OVERVIEW.....	6
2.1	PURPOSE	6
2.2	SCOPE	6
2.3	MANAGEMENT COMMITMENT.....	6
2.4	COORDINATION AMONG ORGANIZATIONAL ENTITIES	6
2.5	COMPLIANCE	6
3	POLICY ROLES AND RESPONSIBILITIES.....	7
3.1	CHIEF INFORMATION SECURITY OFFICER (CISO)	7
3.2	CHIEF PRIVACY OFFICER (CPO)	7
3.3	SECURITY/PRIVACY LEAD	7
3.4	CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL	7
3.5	SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	7
3.6	KENTUCKY ONLINE GATEWAY (KOG) ENTERPRISE IDENTITY MANAGEMENT (EIM) ADMINISTRATORS	8
3.7	SERVICE REQUESTOR	8
4	POLICY REQUIREMENTS	8
4.1	GENERAL INFORMATION	8
4.2	DOMAIN ACCOUNT CREATION	8
4.3	APPLICATION ACCESS.....	9
4.4	NETWORK ACCESS.....	9
4.5	REMOVAL/DELETION OF ACCESS.....	9
4.6	EXTERNAL AUDITOR ACCESS	9
4.7	OFFSHORE ACCESS	10
5	POLICY MAINTENANCE RESPONSIBILITY	10
6	POLICY EXCEPTIONS	10
7	POLICY REVIEW CYCLE.....	10
8	POLICY REFERENCES	10

020.301 CHFS Network-User Account Policy	Current Version: 2.3
020.300 Administrative Security	Review Date: 09/14/2018

1 Policy Definitions

- **Agency:** For the purpose of this document, agency or agencies refers to any department under the Cabinet of CHFS.
- **Confidential Data:** COT standards define confidential data as the data the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Electronic Personal Health Information (ePHI):** Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form.
- **Enterprise Identity Management (EIM):** Identity management solution used to provide internal users with network service entitlements.
- **Federal Tax Information (FTI):** Information received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service, that includes tax information. Examples would be an individual's tax return or anything that the IRS collects and that the IRS is going to use in order to determine a person's tax liability or potential tax liability.
- **Network Access:** Access to servers, Active Directory, databases, folders, within or on the CHFS boundaries.
- **Obfuscated Data:** Data masked or the process of hiding original data within random characters or data sets.
- **Personally Identifiable Information (PII):** Information used to distinguish or trace an individual's identity (i.e. name, Social Security number, biometric records, etc.). PII can be the individual's personal information or is identified when combined with other personal or identifiable information (i.e. date of birth, birthplace, mother's maiden name, etc.).
- **Production Data:** Data within the system that contains citizen's personal, identifiable, sensitive, and confidential information. Data is classified production data if found in any environment and not obfuscated.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)

020.301 CHFS Network-User Account Policy	Current Version: 2.3
020.300 Administrative Security	Review Date: 09/14/2018

- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

020.301 CHFS Network-User Account Policy	Current Version: 2.3
020.300 Administrative Security	Review Date: 09/14/2018

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish a comprehensive level of security controls through a network-user account policy. This document establishes the agency's Network-User Account Policy, to help manage risks and provide guidelines for security best practices regarding network accounts and access.

2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with organizations and/or agencies with the cabinet, which access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

020.301 CHFS Network-User Account Policy	Current Version: 2.3
020.300 Administrative Security	Review Date: 09/14/2018

3 Policy Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible to adhere to this policy.

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

3.3 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

3.4 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section [8 Policy References](#) below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.5 System Data Owner and System Data Administrators

Management/lead who work with the application's development team to document components that are not included in the base server build and ensure functionality and backups are conducted in line with business needs. This individual(s) will be responsible to work with enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

020.301 CHFS Network-User Account Policy	Current Version: 2.3
020.300 Administrative Security	Review Date: 09/14/2018

3.6 Kentucky Online Gateway (KOG) Enterprise Identity Management (EIM) Administrators

Authorized KOG personnel responsible for accepting electronically submitted service requests and submitting them to the Commonwealth Service Desk for completion. These authorized staff personnel are responsible for basic validation of service request information and are listed as an approved IT service contact to submit service desk tickets for CHFS.

3.7 Service Requestor

A CHFS division director approved and is appointed as a designated individual(s) to submit service requests through KOG (i.e. Active Directory (AD), Virtual Private Network (VPN), Home Folder, Shared Folder, Telephone, Enhanced Mailbox, Account, Skype for Business, Other). These designated personnel are responsible to obtain and validate all KOG required information (i.e. user and billing codes) from the CHFS personnel requesting services.

4 Policy Requirements

4.1 General Information

CHFS adheres to Commonwealth Office of Technology (COT) Enterprise Policy: CIO-072- Identity and Access Management Policy. Maintenance of CHFS Domain accounts is coordinated through COT.

The immediate supervisor of a new employee is responsible for ensuring the employee reads and agrees with all information provided through the Office of Human Resource Management (OHRM) Personnel Handbook. CHFS employees must read, understand, and sign the CHFS Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement (CHFS-219) upon initial hire and annually thereafter. The immediate supervisor, or designee, is responsible for requesting the creation, modification, or deletion and employee's CHFS Domain account, as needed, through the Kentucky Online Gateway (KOG).

CHFS staff must coordinate with the KOG team to obtain mainframe user access. Through the KOG Request application, the designated requestor for the user's department shall submit a request for mainframe access and must obtain a CHFS-219B form from the user prior to gaining access to mainframe.

4.2 Domain Account Creation

Newly hired/on boarded state staff are entered into the Human Resource (HR) KHRIS system. Once actions are approved and completed in KHRIS employee data is automatically sent to EIM and the domain account is created. This information is then synced to KOG.

020.301 CHFS Network-User Account Policy	Current Version: 2.3
020.300 Administrative Security	Review Date: 09/14/2018

Newly hired/on boarded contract/vendor staff work with the agency/division's service requestor for a request to create a domain account through KOG. Once KOG receives the request the KOG Administrators manually retain and feed the data into EIM. Once KOG Administrators complete the process, the contract/vendor staff's domain account is created.

4.3 Application Access

Contract, state, and vendor staff requesting application access work with the agency/division's service requestor to submit a request via KOG. The KOG's Request Application Portal is utilized by the Service Requestor for requesting user access. The request is then routed through an automated workflow for approval.

4.4 Network Access

After a state or contract/vendor's account has been created, and if deemed necessary, access to network resources (i.e. database access, server access, etc.) may be requested by appropriate management. The following COT forms must be filled out:

- [F181- Staff Service Request Form](#)
- [F085- Security Exemption Form](#)

When production data/access is being requested, the request forms must be submitted and approved to the OATS IS management for approval. Once completed and CHFS approved, requested must be submitted to CHFSServiceRequests@ky.gov. Please refer to the [COT Forms Page](#) for instructions and additional detailed information.

4.5 Removal/Deletion of Access

For state staff, accounts are removed from EIM once KHRIS actions within HR are completed. Once actions are approved and completed in KHRIS employee data is automatically sent to EIM and synced to KOG for removal. Once information is fed into KOG, the KOG account is marked as inactive.

For contract/vendor staff, accounts to be removed/deleted are requested within the KOG the KOG Administrators manually retain and fed the removal request data into EIM. Once KOG Administrators complete the process the contract/vendor staff's domain account is marked as inactive.

4.6 External Auditor Access

All vendors/auditors must be approved, have business justification and/or agreements in place with the appropriate CHFS agencies to obtain application or network access. Only vendors/auditors deemed appropriate will be approved for minimum necessary access for a defined duration of time. Vendors/auditors are bound by CHFS usage policies and procedures as well as all other federal rules and regulations. Form, CHFS-219V must be completed along with up-to-date antivirus software. External vendor access to any KOG application must follow the steps outlined in the [CHFS External Auditor Access Request Procedure](#).

020.301 CHFS Network-User Account Policy	Current Version: 2.3
020.300 Administrative Security	Review Date: 09/14/2018

4.7 Offshore Access

Production data is prohibited to be accessed by any contract, state, or vendor personnel located offshore. All users requesting production data must be located within the United States. This applies to all CHFS employees, consultants, temporary personnel, contractors, and other entities that interact with CHFS information related resources. By definition, production data is classified as “production data” when located in any environment. If production data is obfuscated, it is then not considered live production data.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

For any staff located within the Department for Behavioral Health, Development, and Intellectual Disabilities (BHDID) who are not on boarded or utilizing KOG, the COT F181EZ Form shall be used to request any action (create, modify, or delete) related to CHFS domain accounts/access. Once forms are completed and approved, they must be submitted to CHFSServiceRequests@ky.gov for completion. Please refer to the COT Forms Page for instructions and more detailed information.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Form: CHFS External Auditor Access Request Form
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Procedure: CHFS External Auditor Access Request Procedure
- CHFS Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement (CHFS-219)
- Enterprise IT Policy: CIO-072- Identity and Access Management Policy

020.301 CHFS Network-User Account Policy	Current Version: 2.3
020.300 Administrative Security	Review Date: 09/14/2018

- Enterprise IT Form Instructions: F181EZ- Staff Service Request, EZ Version, Form Instructions
- Enterprise IT Form: F181EZ- Staff Service Request, EZ Version, Form
- Enterprise IT Form Instructions: F181i- Staff Services Request Form Instructions
- Enterprise IT Form: F181- Staff Service Request Form (and COT Entrance/Exit Form)
- Enterprise IT Form: F085- Security Exemption Request Form
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule: 45CFR164.308(a)(1)(ii)(A)
- Internal Revenue Services (IRS) Publications 1075
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- Kentucky Revised Statute (KRS) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- National Institute of Standards and Technology (NIST) Special Publication 800-66, Rev. 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- Office of Human Resource Management (OHRM) Personnel Handbook
- Social Security Administration (SSA) Security Information